EXHIBIT A
TO
NOTICE OF REMOVAL

KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN 249203)
ak@kazlg.com
Mona Amini (SBN 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff,
Sarvenaz Safai

Assigned for All Purposes
Judge Peter Wilson

CX-102

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ORANGE – COMPLEX CIVIL

SARAVENAZ SAFAI, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

FLAGSTAR BANKCORP, INC.; FLAGSTAR BANK, FSB; and DOES 1-50, Inclusive,

Defendants.

Case No.: 30-2022-01266908-CU-NP-CXC

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*; and
3. BREACH OF CONTRACT

JURY TRIAL DEMANDED

KAZEROUNI LAW GROUP, APC

//

//

//

//

//

//

//

//

Plaintiff SARVENAZ SAFAI ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class members"), by and through Plaintiff's attorneys, upon personal knowledge as to facts pertaining to herself and on information and belief as to all other matters, brings this class action against FLAGSTAR BANKCORP, INC.; FLAGSTAR BANK, FSB; and DOES 1-50, Inclusive (collectively "Flagstar" or "Defendants"), and alleges as follows:

NATURE OF THE CASE

1. This is a data breach class action arising out of Flagstar's failure to implement and maintain reasonable security practices to protect consumers' sensitive personal information. Flagstar is a national bank that offers full-service banking and lending. "Flagstar has assets of $23.2 billion, is the sixth largest bank mortgage originator nationally, and the second largest savings bank in the country."[1] For its business purposes, Flagstar obtains, stores, and transmits personally identifiable information ("PII") related to its customers, including but not limited to names, addresses, Social Security Numbers, financial information (e.g., account numbers, credit, or debit card numbers), and other types of information.

2. On or around June 2, 2022, Flagstar learned that between December 3, 2021, and December 4, 2021, an unauthorized party accessed Flagstar's network and accessed and/or acquired files containing Plaintiff's and other Class members' personal information (the "Data Breach"). Flagstar determined that the Data Breach impacted files containing Plaintiff's and the Class members' Social Security number, account/loan number, name, address, date of birth, and financial institution name. While the exact number of affected customers is presently unknown, based upon information and belief, over 1.5 million customers have been affected by the Data Breach.

3. Although the Data Breach occurred between December 3 and December 4, 2021, and Flagstar knew or should have known that sensitive personal information of its customers was accessed and exfiltrated by unauthorized persons and in the hands of malicious actors, Flagstar waited until on or around June 16, 2022, to send customers affected by the Data Breach letters informing them of the unauthorized access to their personal information. Flagstar's notice to

[1] https://www.flagstar.com/about-flagstar.html

customers was misleading and inadequate as the notice did not provide the details of the Data Breach or explain the delay between the breach and notifying affected customers.

4. The Data Breach occurred as a result of Flagstar's inadequate cybersecurity, which caused Plaintiff's and Class members' PII to be accessed, exfiltrated, and disclosed to unauthorized persons. This action seeks to remedy these failings. Plaintiff brings this action on behalf of herself and all affected California residents.

5. As set forth in the Prayer for Relief, among other things, Plaintiff seeks, for herself and the Class members injunctive relief, including public injunctive relief, and actual damages.

VENUE AND JURISDICTION

6. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiff and the Class members pursuant to Cal. Code Civ. Proc. § 382.

7. This Court has personal jurisdiction over Flagstar because Flagstar regularly conducts business in California and is headquartered in San Diego, California.

8. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. § 395 and § 395.5 because Flagstar regularly conducts business in the State of California, and the unlawful acts or omissions giving rise to this action also occurred or arose in this county.

PARTIES

9. At all relevant times, Plaintiff resided in the State of California.

10. At all relevant times, Flagstar conducted business in the State of California.

11. Plaintiff provided her PII to Flagstar, including but not limited to Plaintiff's name, address, date of birth, and Social Security Number. In June 2022, Plaintiff learned that her PII was accessed and/or acquired by unauthorized individuals through the Data Breach.

12. Flagstar sent Plaintiff a letter dated June 16, 2022, with the title "*NOTICE OF DATA BREACH*." The letter notified Plaintiff and similarly situated persons that as a result of the Data Breach there was unauthorized actor to Flagstar's network and an unauthorized actor accessed and/or acquired files containing Flagstar's customers' personal information, including but not limited to Social Security number, account/loan number, name, address, date of birth, and financial

institution name. No details were provided regarding how or who accessed or stole the information or why there was a delay in notifying affected customers.

13. As a result of Flagstar's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected, maintained, and stored on its servers, network, and/or email system, Plaintiff's PII was accessed, viewed, exfiltrated, stolen and/or otherwise disclosed to unauthorized persons in the Data Breach.

14. Defendant Flagstar Bancorp, Inc. is a domestic corporation formed under the laws of the State of Michigan with a headquarters located in Troy, Michigan.

15. Defendant Flagstar Bank, FSB is a domestic corporation formed under the laws of the State of Michigan with a headquarters located in Troy, Michigan. Flagstar Bank is a subsidiary of Flagstar Bancorp, Inc.

16. Plaintiff is unaware of the true names and capacities of the Defendants sued herein as DOES 1 through 50, inclusive, and therefore sues this Defendants by such fictitious names pursuant to Cal. Civ. Proc. Code § 474. Plaintiff is informed and believes, and based thereon, alleges that Defendants designated herein are legally responsible in some manner for the unlawful acts and occurrences complained of herein, whether such acts were committed intentionally, negligently, recklessly, or otherwise, and Defendants thereby proximately caused the injuries and damages to Plaintiff and the Class members as herein alleged. Plaintiff will seek leave of Court to amend this complaint to reflect the true names and capacities of Defendants when they have been ascertained and become known.

17. The agents, servants and/or employees of Defendants and each of them acting on behalf of Defendants acted within the course and scope of his, her or its authority as the agent, servant and/or employee of Defendants, and personally participated in the conduct alleged herein on behalf of Defendants with respect to the conduct alleged herein. Consequently, the acts of each of the Defendants are legally attributable to the other Defendants and all Defendants are jointly and severally liable to Plaintiff and other similarly situated individuals, for the loss sustained as a proximate result of the conduct of the Defendants' agents, servants and/or employees.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

18. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.[2] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

19. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[3]

20. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[4] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

21. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[5]

22. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the

---

[2] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[3] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[4] *See* Soma, *Corporate Privacy Trend, supra*.

[5] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

23. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[6] This business has created a new market for the sale and purchase of this valuable data.[7]

24. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[8]

25. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[9]

26. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[6] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/ 18unboxed.html.

[7] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[8] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1# page_scan_tab_contents.

[9] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

Theft of PII Has Grave and Lasting Consequences for Victims

27. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

28. Theft or breach of PII is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[10]

29. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[11] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

30. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[12]

31. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[13] According to Experian, "[t]he research

---

[10] California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

[11] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

[12] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[13] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[14]

32. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[15] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[16] And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[17]

33. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

34. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[18]

---

[14] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[15] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[16] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

[17] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[18] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

35. It is within this context that Plaintiff and over 1.5 million of Flagstar's customers face imminent risk of identity theft and must now live with the knowledge that their PII is forever in cyberspace and was accessed and taken by unauthorized persons willing and able to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web or the black market for other malicious actors.

Flagstar's Business

36. Flagstar is a bank headquartered in Troy, Michigan with numerous locations across the United States. Flagstar operates 150 branches throughout 150 branches in Michigan, Indiana, California, Wisconsin, and Ohio, and is the sixth largest bank mortgage originator nationally, and the second largest savings bank in the country.[19]

37. When Plaintiff and similarly situated customers applied for accounts or financing with or through Flagstar, they were required to provide Flagstar with certain personal information. This personal information includes the customer's name, Social Security Number, date of birth, and other personal information.

Flagstar's Collection of Customers' PII

38. Flagstar acknowledges that they obtain, store and transmit a substantial amount of personal and financial information from its customers. The type of information is detailed in Flagstar's Privacy Policy (last revised February 2018),[20] which states that Flagstar collects and shares the following categories of personal information from customers:

- Social Security number and credit scores
- Account transactions and checking account information
- Transaction history and payment history

39. Flagstar collects personal information from customers that they voluntarily provide in various ways, including when customers open an account or deposit money, when they pay bills or apply for a loan, or when they use their debit card.

---

[19] https://www.flagstar.com/about-flagstar.html

[20] https://www.flagstar.com/content/dam/flagstar/pdfs/about-flagstar/PrivacyPolicy.pdf

40. For California customers, Flagstar's California Privacy Notice & Policy identifies the rights of California residents regarding their personal information pursuant to the California Consumer Privacy Act ("CCPA").[21] These rights include requesting disclosure of the information collected, the purpose for collecting the information, and any third parties with whom the information is sold or disclosed. Additionally, the rights under the CCPA identified by Flagstar's Privacy Policy include requesting deletion of the personal information, opting out of have personal information sold to third parties, and receiving information that identifies any third party that has received personal information.

41. Flagstar's CCPA Privacy Policy also sets forth the categories of personal information Flagstar collects. This includes the following: identifiers (*e.g.,* name, address, Internet Protocol address, email address, account name, Social Security Number, driver's license number, passport number); Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) (*e.g.,* name, signature, Social Security number, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, bank account number, credit or debit card number, medical information, or health insurance information); commercial information (*e.g.,* personal property, purchasing or consuming history); biometric information (*e.g.,* fingerprints, facial recognition); Internet or network activity (*e.g.,* browsing history, search information, consumer interaction with website, application, or advertisement); geolocation data; (*e.g.,* physical location or movements); and sensory data, such as audio.

Flagstar's Promises to Safeguard Customer PII

42. Flagstar claims it has "built processes to identify cybersecurity threats and ensure our data and customer privacy are well-protected. These processes have been built in partnership with Flagstar's Chief Risk Officer, Chief Information Officer, business unit leaders, and enterprise risk management team."[22]

43. Flagstar's Terms of Use Agreement expressly references Flagstar's Privacy Statement.

---

[21] https://www.flagstar.com/legal-disclaimers/ccpa-privacy-notice.html

[22] h https://www.flagstar.com/esg/governance/data-security-and-customer-privacy.html

Flagstar's Notice of Data Breach

44. On June 16, 2022, Flagstar sent Plaintiff and other similarly situated customers a letter with the title, "Notice of Data Breach" The letter states that "Flagstar Bank treats the security and privacy of your personal information with the utmost importance, which is why we are writing to let you know about a recent security incident."

45. The letter goes on to state that Flagstar discovered on June 2, 2022, that certain impacted files containing Plaintiff and the Class members' personal information were accessed and/or acquired from Flagstar's network between December 3, 2021, and December 4, 2021.

46. According to Flagstar, the accessed and exfiltrated information included Plaintiff's name and unencrypted Social Security Number, account/loan number, date of birth, and financial institution name, among other personal information.

47. Flagstar offered customers a two-year complimentary membership to Kroll's identity monitoring program.

48. Additionally, Flagstar offered a limited number of steps on how to protect against identity theft and fraud. These steps included reviewing financial account statements and credit reports.

49. Flagstar's letter did not identify the rights of consumers under CCPA for California residents.

50. Pursuant to California Civ. Code § 1798.82(a)(1), data breach notification letters must be sent to residents of California "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]"

51. Plaintiff's and Class members' PII is "personal information" as defined by California Civ. Code § 1798.82(h).

52. California Civ. Code § 1798.82(g) defines "breach of the security of the system" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."

53. The Data Breach was a "breach of the security of the system" as defined by California Civ. Code § 1798.82(g).

54. Thus, Flagstar filed and disseminated its breach notification because Plaintiff's and Class members' unencrypted personal information was accessed and acquired by an unauthorized person or persons as a result of the Data Breach.

55. Flagstar's Notice of the Data Breach letter sent to Plaintiff and other putative class members is inadequate and fails to provide sufficient detail. Flagstar states only that it discovered on June 2, 2022, that certain impacted files containing Plaintiff and the Class members' personal information was accessed and/or acquired between December 3, 2021, and December 4, 2021. It is unclear whether the intrusion, or intrusions, occurred on two consecutive days or two separate days or every day, how the Data Breach occurred, or why it took six (6) months for Flagstar to discover the Data Breach.

56. Flagstar's vague description of the Data Breach leaves Plaintiff and Class members at continuing risk. By failing to adequately inform Plaintiff and Class members of the details surrounding the breach Plaintiff and Class members are unable to adequately protect themselves against identity theft and other damages.

57. Further, Flagstar offer Plaintiff and Class members little to assist them with any fall-out from the Data Breach or to advise them of the extent of the potential threat they face as a result of their sensitive PII being in the hands of criminals. Flagstar offer of a two-year subscription to Kroll's identity theft protection program is insufficient where Plaintiff and Class members are now at increased and imminent risk of identity theft for years to come as a result of the Data Breach.

58. Flagstar's "Notice of Data Breach" letter also fails to explain why it took months for it to realize that the Data Breach had occurred or any explanation for the delay in notifying Plaintiff and Class members about the Data Breach. This delayed Plaintiff's and Class members' ability to take necessary precautions to protect themselves from identity theft and other fraud.

//

//

//

Flagstar Knew or Should Have Known PII Are High Risk Targets

59. Flagstar knew or should have known that PII like the information obtained, maintained, and stored on Flagstar's servers and network, including its email system, is a high-risk target for identity thieves.

60. The Identity Theft Resource Center reported that the business sector had the largest number of breaches in 2018. According to the ITRC this sector suffered 571 data breaches exposing at least 415,233,143 million records in 2018.[23] Further, the ITRC identified "hacking" as the most common form of data breach in 2018, accounting for 39% of data breaches.

61. Prior to the Data Breach, there were many reports of high-profile data breaches that should have put a company like Flagstar on high alert and forced it to closely examine their own security procedures, as well as those of third parties with which it did business and gave access to their subscriber PII.

62. As such, Flagstar was aware that PII is at high risk of theft, and consequently should have, but did not, take appropriate and standard measures to protect Plaintiff's and Class members' PII against cyber-security attacks, unauthorized access, and disclosure that Flagstar should have anticipated and guarded against.

CLASS DEFINITION AND ALLEGATIONS

63. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiff seeks to represent and intends to certify a class defined as (the "Class"):

> All California residents who Flagstar and/or its agents sent a "Notice of Data Breach" letter informing them their personally identifiable information (PII) was subjected to the Data Breach.

64. Excluded from the Class are: (1) Flagstar and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such

[23] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

65. Certification of Plaintiff's claims for classwide treatment is appropriate because Plaintiff can prove the elements of her claims on a classwide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

66. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, Flagstar acknowledges the Data Breach, and reports estimate the breach to include over 1.5 million customers, including Plaintiff and Class members. Thus, Plaintiff believes that the Class is so numerous that joinder of all members is impractical.

67. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

68. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Flagstar had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected from Plaintiff and Class members;

(b) Whether Flagstar breached their duty to protect the PII of Plaintiff and each Class member; and

(c) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

69. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that Plaintiff has no interests adverse to or that

conflicts with the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

70. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

71. Flagstar has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code §§ 1798.100, *et seq.*

72. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

73. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time

and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[24]

74. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Flagstar failed to implement such procedures which resulted in the Data Breach.

75. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

76. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

77. Plaintiff and Class members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

78. Flagstar is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

---

[24] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

(a) is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

(b) "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

(c) does business in California; and

(d) has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

79. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and Class members' name and unencrypted Social Security Number, among other information.

80. Plaintiff's and the putative Class' PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized third parties.

81. The Data Breach occurred as a result of Flagstar's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Flagstar failed to implement reasonable security procedures to prevent an attack on their server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff's and Class members' PII as a result of this attack.

82. On or around June 27, 2022, Plaintiff provided Flagstar with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Exhibit A. If Flagstar does not cure the violation within 30 days, Plaintiff will amend the complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

- 25 -

EXHIBT A

83. As a result of Flagstar's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks actual damages, injunctive relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION

Violation of the California Unfair Competition Law ("UCL")

(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)

84. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

85. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Flagstar engaged in unlawful, unfair, and fraudulent practices within the meaning, and in violation of, the UCL.

86. In the course of conducting their business, Flagstar committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq*.) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiff and Class members reserve the right to allege other violations of law by Flagstar constituting other unlawful business acts or practices. Flagstar's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

87. Flagstar also violated the UCL's unlawful prong by breaching contractual obligations created by their Privacy Policies and by knowingly and willfully or, in the alternative, negligently and materially violating Cal. Bus. & Prof. Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply

with the provisions of their posted privacy policy. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Flagstar's violations of their Privacy Policies.

88. Flagstar also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

89. Flagstar's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Flagstar's wrongful conduct is substantially injurious to consumers, offends legislatively declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Flagstar's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Flagstar's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Flagstar's legitimate business interests other than engaging in the above-described wrongful conduct.

90. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Flagstar's violations of their Privacy Policies and statutory and common law in that a portion of the money Plaintiff and Class members paid for Flagstar's products and services went to fulfill the contractual obligations set forth in their Privacy Policy, including maintaining the security of their PII, and Flagstar's legal obligations and Flagstar failed to fulfill those obligations.

91. The UCL also prohibits any "fraudulent business act or practice." Flagstar's above-described claims, nondisclosures and misleading statements were false, misleading, and likely to deceive the consuming public in violation of the UCL.

92. As a direct and proximate result of Flagstar's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost

money or property as a result of Flagstar unfair and deceptive conduct. Such injury includes paying for a certain level of security for their PII but receiving a lower level, paying more for Flagstar's products and services than they otherwise would have had they known Flagstar was not providing the reasonable security represented in their Privacy Policy and as in conformance with their legal obligations. Had Plaintiff and Class members known about Flagstar's substandard data security practices they would not have purchased Flagstar's products or services or would have paid less for them. Flagstar's security practices have economic value in that reasonable security practices reduce the risk of theft of customer's PII.

93. Plaintiff and Class members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) damages under the CCPA, (v) deprivation of the value of their PII, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

94. Unless restrained and enjoined, Flagstar will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Flagstar from continuing such wrongful conduct, and requiring Flagstar to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

//

//

//

//

FOURTH CAUSE OF ACTION

Breach of Contract

95. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

96. Plaintiff and Class members entered into express contracts with Flagstar as set forth in their Terms of Use and Privacy Policy that included Flagstar's promise to protect nonpublic personal information given to Flagstar or that Flagstar gathered on their own, from disclosure, as set forth in Flagstar's Privacy Policy, which was posted on its website.

97. Plaintiff and Class members performed their obligations under the contracts when they provided their PII to Flagstar in relation to their purchase of insurance products or services from Flagstar.

98. By allowing unauthorized users to gain access to Plaintiff's and Class members' PII through the Data Breach, Flagstar breached these contractual obligations. As a result, Flagstar failed to comply with their own policies, including their Privacy Policies, and applicable laws, regulations and industry standards for data security and protecting the confidentiality of PII. Flagstar's breach of contract also violated California Business and Professions Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of their posted privacy policy.

99. By failing to fulfill their contractual obligations under their Terms of Use and Privacy Policy, Flagstar failed to confer on Plaintiff and Class members the benefit of the bargain, causing them economic injury.

100. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all members of the Class respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated representative of the Class, and (iii) Plaintiff's undersigned counsel be appointed as Class Counsel.

Plaintiff, on behalf of herself and members of the Class further requests that upon final trial or hearing, judgment be awarded against Flagstar for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) statutory damages;

(iii) equitable relief, including restitution;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit;

(vii) pre- and post-judgment interest at the highest legal rates applicable; and

(viii) any such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself individually and the putative class, hereby demands a jury trial on all issues so triable.

Dated: June 27, 2022

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: _____

Abbas Kazerounian, Esq.
Mona Amini, Esq.
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff Sarvenaz Safai and the putative class

EXHIBIT A

KAZEROUNI LAW GROUP, APC

245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

June 27, 2022

VIA CERTIFIED MAIL
Flagstar Bancorp, Inc. and Flagstar Bank, FSB
5151 Corporate Drive
Troy, Michigan 48098

Re: Sarvenaz Safai v. Flagstar Bank, et al

To Whom It May Concern:

We represent Plaintiff Sarvenaz Safai ("Plaintiff") and all other similarly situated consumers in a putative class action against Flagstar Bancorp, Inc. and Flagstar Bank, FSB (collectively "Flagstar" or "Defendants") arising out of, *inter alia*, Flagstar's failure to provide reasonable security for Plaintiff's and the proposed Class members' personal information, which resulted in the unauthorized access, theft, or disclosure of this information (the "Data Breach"). To our knowledge the Data Breach occurred on between December 3 and December 4, 2021, as specified in Flagstar's "Notice of Data Breach" letter to Plaintiff dated June 16, 2022.

The full claims, including the facts and circumstances surrounding these claims are detailed in Plaintiff's Class Action Complaint, a copy of which is attached and incorporated by reference. Flagstar's conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of the claims asserted against Flagstar, pursuant to California Civil Code 1798.150(b)(1), Plaintiff demands that, in the event a cure is possible, Flagstar is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiff with an express written statement within 30 days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiff and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/ Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]